

Forum:[Hack Forums](#)

Thread: [Bitchat \(Bluetooth Mesh Chat\)](#)

Omniscient - July 25, 2026, 11:25 am

I don't see any threads on HF about Bitchat. I'm going to just copy the content from the official site. Project created by Jack Dorsey (Twitter Founder). It's amazing.

<https://bitchat.free/>

bitchat is a decentralized peer-to-peer messaging application that operates over Bluetooth mesh networks.

No internet required. No servers. No phone numbers.

Traditional messaging applications depend on centralized infrastructure that can be monitored, censored, or disabled.

bitchat creates ad-hoc communication networks using only the devices present within physical proximity. Each device acts as both a client and server, automatically discovering peers and relaying messages across multiple hops to extend the network's reach.

This approach provides censorship resistance, surveillance resistance, and infrastructure independence.

The network remains functional during:
Internet outages

Natural disasters

Protests

Regions with limited connectivity

Software

iOS and macOS Version

App Store:
[bitchat mesh](#)

Source Code:
github.com/permissionlesstech/bitchat

Supports iOS 16.0 or newer and macOS 13.0 or newer.

The application can be built using Xcode with XcodeGen or Swift Package Manager.

Android Version

Google Play Store:
[bitchat](#)

Source Code:
github.com/permissionlesstech/bitchat-android

APK Releases:
github.com/permissionlesstech/bitchat-android/releases

Supports Android 8.0 or newer, API level 26 or higher.

The Android version provides full protocol compatibility with the iOS version.

Documentation

Technical Whitepaper:
[WHITEPAPER.md](#)

The software has been released into the public domain.

Permissionless Tech

Mr.Cat - July 25, 2026, 11:31 am

i still dont understand how it works.. singlal wise.. So like via bluetooth? Moblile Data?

Omniscient - July 25, 2026, 11:51 am

(Jul 25, 2026 11:31 AM)Mr.Cat Wrote: [\[CITE\]](#) i still dont understand how it works.. singlal wise.. So like via bluetooth? Moblile Data?

No mobile data or internet required. It's bluetooth mesh.

Basically unstoppable and zero surveillance.

Mr.Cat - July 25, 2026, 12:07 pm

(Jul 25, 2026 11:51 AM)Omniscient Wrote: [\[CITE\]](#) No mobile data or internet required. It's bluetooth mesh.

Basically unstoppable and zero surveillance.

i think is a cool idea if enouph people use it and buetooth jumps from person to person for the range to be increased.. but what about attacks like man in the middle and stuff like that since you cant create private rooms to talk to someone specifically

Omniscient - July 25, 2026, 12:19 pm

(Jul 25, 2026 12:07 PM)Mr.Cat Wrote: [\[CITE\]](#) i think is a cool idea if enouph people use it and buetooth jumps from person to person for the range to be increased.. but what about attacks like man in the middle and stuff like that since you cant create private rooms to talk to someone

specifically

Good question. I had to ask AI.

AI Quote: Bitchat uses Noise Protocol encryption, but it does not automatically eliminate a man-in-the-middle attack during first contact.

For private Bluetooth conversations, it uses:

`Noise\_XX\_25519\_ChaChaPoly\_SHA256`

The Noise XX handshake:

- Generates temporary session keys.

- Exchanges each device's persistent public identity key. Derives separate encrypted transport keys.

- Uses ChaCha20-Poly1305 to detect modification and encrypt messages.

- * Provides forward secrecy, so later theft of a long-term identity key should not expose previous session traffic. ([GitHub][1])

This prevents ordinary mesh relay devices from reading or silently modifying private messages. Intermediate phones forward encrypted packets; they do not possess the conversation's end-to-end session keys. ([GitHub][1])

The important limitation

Noise XX authenticates cryptographic keys, but on first contact it does not inherently prove that a key belongs to the person whose nickname you see.

An active attacker positioned between Alice and Bob could theoretically:

1. Establish one encrypted session with Alice.
2. Establish a separate encrypted session with Bob.
3. Present their own key to each side.
4. Decrypt and re-encrypt messages between them.

Both connections would be encrypted, but each would terminate at the attacker.

Bitchat addresses this through fingerprint verification. Every identity has a fingerprint calculated from its long-term Curve25519 public key:

`SHA-256(Noise static public key)`

Users must compare that fingerprint through a separate trusted method—ideally in person, by QR code, over a trusted call, or through another authenticated channel—and then mark the contact as verified. ([GitHub][1])

Once you have verified and saved the correct fingerprint, an attacker presenting a different identity key can be detected. The project's own whitepaper explicitly says that users must verify fingerprints out-of-band to prevent MITM attacks. ([GitHub][1])

So the accurate description is:

> Bitchat prevents passive interception and protects messages from mesh relays automatically. Full protection against an active first-contact MITM requires users to compare and verify identity fingerprints.

Simply recognizing the username is not enough because nicknames are not inherently trustworthy or unique.

[1]:

https://github.com/permissionlesstech/bitchat/blob/main/WHITEPAPER.md?utm_source=chatgpt.com "WHITEPAPER.md - permissionlesstech/bitchat"

Raijin - July 25, 2026, 3:14 pm

Wow this is a cool looking piece of new technology. Thanks.

7 - July 25, 2026, 9:31 pm

It's like a bluetooth version of Chinese whispers... maybe that would be a fun version of it.

Palestine - July 30, 2026, 5:10 am

Isn't this what they did in the show "The Last Ship"? They were able to communicate P2P with just Bluetooth and no cell towers.

Binance - July 30, 2026, 8:12 am

Very cool.

But I, like many others, don't have privacy conscious friends irl that I'm close enough to use this with.

Isolate - July 31, 2026, 12:29 am

I can see how this might be useful for some people but at the same time I feel like something like this opens the door for a more targeted attack.

I am sure there is some sort of safeguards in place to prevent frequency hijacking's but I am curious if they are able to target a device that is connected to a network and is close enough to devices running bitchat to provide a connection point for a some sort of frequency manipulation or hijacking to allow them to pick up that signal read and send messages on the network.

At the same time I wonder if that could be used an implementation or 3rd party software to be able to invite users into these chats for short periods of time before disabling the connection again to the carriers number like a switch.

I mean all theoretical but I feel still very plausible in today's technology.

HALx86 - August 2, 2026, 1:59 pm

I haven't used it but I have it downloaded. I love the idea of it. Unfortunately, I think it's one of those things that needs a big adoption to be useful.

It looks like there's been moves by some governments to have it removed from the store --
<https://www.yahoo.com/news/articles/jack-dorsey-bitchat-removed-apple-130800888.html>

TheJohnnyDepp - *August 3, 2026, 2:01 am*

Neat project! Thank you for the share. Always nice to see new chat programs with good privacy in development. I'm not a fan of the current offerings.

Rahul007rhp - *August 5, 2026, 11:06 am*

Such a dope tech project. Thanks for posting

CyberXero - *August 15, 2026, 3:44 pm*

Bitmesh.. damn that's great, but surely there is a way to intercept these packets, overall bitmesh sounds like it's gonna be something big, but is there a distance limit?